

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-53968

(P2004-53968A)

(43) 公開日 平成16年2月19日(2004.2.19)

(51) Int.Cl.⁷G 0 9 C 1/04
H 0 4 L 9/28

F 1

G 0 9 C 1/04
H 0 4 L 9/00 6 6 1

テーマコード(参考)

5 J 1 O 4

審査請求 有 請求項の数 7 O L (全 7 頁)

(21) 出願番号

特願2002-211930(P2002-211930)

(22) 出願日

平成14年7月22日(2002.7.22)

(71) 出願人

500401453
グローバルフレンドシップ株式会社
東京都新宿区四谷四丁目13番地

(74) 代理人

100104341

弁理士 関 正治

(72) 発明者

保倉 豊

東京都渋谷区幡ヶ谷1-11-13-50
6

F ターム(参考) 5J104 AA12 PA07

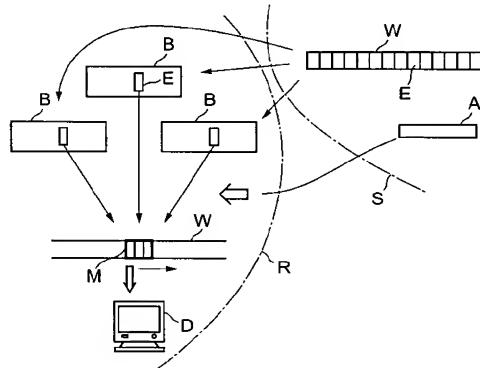
(54) 【発明の名称】電子情報送信システム

(57) 【要約】

【課題】大量の電子情報を安全に送付でき、特に、ストリーミング型通信によりコンテンツを送付する場合に効率的に使用することができる秘密分散法を活用した電子情報送信システムを提供する。

【解決手段】発信元Sで元の電子情報Wを秘密分散法で複数の情報ブロックBに分割して送信し、受信者Rが受信した情報ブロックBに含まれる情報エレメントEの配列を元に戻して電子情報Wを復元して再生するもので、発信元コンピュータSが情報エレメントEの順序と所在を記録した配列情報Aを作成して送信し、受信者コンピュータRが配列情報Aに基づいて所定の時間幅に存在する情報エレメントEを収集し電子情報を復元してバッファメモリMに記録し、電子情報を再生すると次に順が来る情報エレメントEを収集して電子情報を復元しバッファメモリMに補填し、常時ほぼ一定量の電子情報を保持して復元可能にする。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

発信元におけるコンピュータが元の電子情報を任意の数の情報エレメントに分割して、少なくとも2個の情報ロックに分類し、それぞれの情報ロックにおいて属する情報エレメントを任意の順に配列して、受信者のコンピュータに送信し、受信者のコンピュータが該情報ロックを受信し、情報ロックの配列と各情報ロックに含まれる情報エレメントの配列を元に戻して元の電子情報を復元して再生するようにした電子割符式電子情報送信システムにおいて、発信元のコンピュータが前記情報エレメントの時系列的な順序と所在を記録した配列情報を作成して受信者のコンピュータに送信し、受信者のコンピュータが該配列情報を基づいて所定の時間幅の情報エレメントを収集して含まれる電子情報を復元し、復元した電子情報をバッファメモリに記録し、該バッファメモリに格納された電子情報を再生するときには再生された電子情報をバッファメモリから消去し、次に順が来る情報エレメントについて電子情報を復元してバッファメモリに補填し常時ほぼ一定量の電子情報を保持するようにしたことを特徴とする電子情報送信システム。10

【請求項 2】

前記情報ロックに含まれる情報エレメントは互いに元の電子情報の中で近傍に位置するものであることを特徴とする請求項1記載の電子情報送信システム。

【請求項 3】

前記配列情報は、任意の数の情報エレメントに分割してロックに分配し使用するときに収集して復元するようにすることを特徴とする請求項1または2に記載の電子情報送信システム。20

【請求項 4】

前記情報ロックの少なくとも1個は、発信元のコンピュータに保留されていて受信者が発信元の認証を得たときに初めて送付されることを特徴とする請求項1から3のいずれかに記載の電子情報送信システム。

【請求項 5】

前記情報ロックは予め受信者の元に配信されることを特徴とする請求項1から3のいずれかに記載の電子情報送信システム。

【請求項 6】

前記配列情報は情報ロックごとに付属させるヘッダに埋込まれて送信されることを特徴とする請求項1から3のいずれかに記載の電子情報送信システム。30

【請求項 7】

前記情報ロックは少なくとも1個を除き、予め受信者の元に配信されることを特徴とする請求項6記載の電子情報送信システム。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、電子情報を送付するときに安全に送付できる電子情報送信システムに関し、特にストリーミング型通信によりコンテンツを送付する場合に有効に使用することができる電子情報送信システムに関する。40

【0002】**【従来の技術】**

本願発明者が特願2000-596548、国際出願公開公報WO00/45858などによって既に開示した電子割符方法によれば、容量が限られた一塊のファイルや情報を安全に送付することができる。この電子割符方法は秘密分散法の1種と見ることができ、電子情報の全体を分割しランダムに組合わせて別々に送信し、受信者側では送信ロックを全部受信してから割符情報によって統合し元の情報を復元するものである。

この方法で送信すると、送信中の情報ロックの一部を入手してもそれだけでは元の情報の一部といえども復元することができます、情報の窃取を防止することができます。また、この電子割符法を利用すれば、一部の電子情報を予め受信者側に配布しておいて、購読契約50

が成立した者にのみ残りの電子情報をインターネット経由で送って再生させるようすれば、正規の購入者以外に利用されることなく、また確実に課金することができます。このように電子割符法は、有価の情報を安全に送信する場合や、著作権を保護したい場合に有効である。

【0008】

ところで、たとえば音声、ビデオ、アニメーションなど容量の大きいデータを閲覧する場合には、全てのデータを受信してから再生するのではなく、受信した順にすぐ再生をするようにしたストリーミング技術が用いられる。このようなストリーミング技術を使用する場合は、受信した部分から逐次再生してもそれぞれの部分で意味のある情報になっている必要がある。

10

しかし、電子情報の全体を受信してから復元する方式である電子割符手段は、情報全体を受信してから一挙に再生するので、情報量の大きいコンテンツを伝送するときには待ち時間が長大になりすぎ、また、再生に使用するコンピュータに膨大な容量の記憶装置が必要になる。したがって、ストリーミングなど大容量の情報伝送をするとときには、安全性が高い電子割符手段を用いることに制約があった。

【0004】

【発明が解決しようとする課題】

そこで、本発明が解決しようとする課題は、大量の電子情報を安全に送付できる電子割符を用いた電子情報送信システムを提供することであり、特に、ストリーミング型通信によりコンテンツを送付する場合に有効に使用することができる電子情報送信システムを提供することである。

20

【0005】

【課題を解決するための手段】

上記課題を解決するため、本発明の電子情報配信システムは、発信元におけるコンピュータが元の電子情報を任意の数の情報エレメントに分割して、少なくとも2個の情報ブロックに分類し、それぞれの情報ブロックにおいて属する情報エレメントを任意の順に配列して、受信者のコンピュータに送信し、受信者のコンピュータがその情報ブロックを受信し、情報ブロックの配列と各情報ブロックに含まれる情報エレメントの配列を元に戻して元の電子情報に復元して再生するようにした動的電子割符式電子情報送信システムである。

30

【0006】

本発明の電子情報送信システムでは、発信元のコンピュータが情報エレメントの時系列的な順序と所在を記録した配列情報を作成して受信者のコンピュータに送信する。一方、受信者のコンピュータが受信した配列情報を基づいて所定の時間幅に存在する情報エレメントを抽出し、情報エレメントに含まれる電子情報を復元し、復元した電子情報をバッファメモリに記録し、バッファメモリに格納された電子情報を再生するときには再生された電子情報をバッファメモリから消去し、次に順が来る情報エレメントについて電子情報を復元してバッファメモリに補填して、常時ほぼ一定量の電子情報を保持するようにしたことを特徴とする。

【0007】

本発明によれば、配列情報をそれぞれの情報エレメントの順序を記録してあるので、受信者のコンピュータが配列情報を取得することにより、どの情報ブロックのどこに存在する情報エレメントを集めれば必要な時間帯の電子情報を順次収集することができるかが分る。したがって、初めに5分とか10分間など適当な時間幅について情報復元をしてバッファメモリに蓄えておくことにより、断裂等することなく看者にストレスを感じさせることなくストリーム情報を再生させることができる。バッファメモリに蓄えた情報は読み捨てて従って、それに続く時間分の電子情報を新たに収集し復元して補填することができる。配列情報は、発信元のコンピュータが受信者のコンピュータに供給して始めて利用することができる。このため、一部の電子情報が漏洩しても配列情報が無い限り再生できないので情報は安全に保護される。

40

【0008】

50

なお、本発明の電子情報送信システムにおいて、それぞれの情報ブロックに亘りに元の電子情報の中で近傍に位置する情報エレメントを集めようとしてもよい。このような情報ブロックを用いると、電子情報の再生に従って収集する情報エレメントはごく少数の情報ブロックに分散して包含されるので、収集に便利であり、またある時間帯について復元処理した後は同じ情報ブロックを再使用する必要がないので、その部分を廃棄することができます。

このような情報ブロックは、発信元のコンピュータがストリームに従って順次電子情報を供給するようなシステムにおいても、有効に利用することができます。なお、隣同士の情報ブロックに配分する情報エレメントの前後関係が多少入混じっていてもよいことはいうまでもない。

【0009】

発信元のコンピュータは、情報ブロックの少なくとも1個を保留して、残りの情報ブロックを予め受信者の元に配信しておき、受信者から使用の申込みを受けたときに初めて保留しておいた情報ブロックを送付するようにしてもよい。

情報ブロックが欠如すると電子情報の復元ができないので、真正な権利者以外には電子情報の利用を行うことができず電子情報の安全が保持できる。

また、電子情報の極く僅かな部分だけを送信すればよいので、電子情報再生時ににおけるアクセスによって通信網に過大な負荷を与えることを排除して、情報配信業者の負担を軽減することができる。

【0010】

なお、情報ブロックは、受信者のコンピュータが電子情報を再生するときに通信回路網を利用して発信元のコンピュータから逐次送信してもよいが、予め通信網を介して、あるいはDVDやCDなど別の媒体で配布あるいは送付しておいてもよい。

発信元は、たとえばインターネットウェブからのダウンロード、雑誌の付録、ダイレクトメール、路上の配布などを介して音楽、映画、アニメなどのコンテンツを含む電子情報を配布する。この電子情報は情報ブロックを含むが、秘密分散技術で電子情報を復元できないように処理されている。ただし、電子情報から抽出した一部の試供部分については秘密分散処理をしないでそのまま再生できるようにしてある。

【0011】

需要者は電子情報の一部を確認した上で、インターネットなどを介してその購入を申込むと初めて配列情報や残りの情報ブロックを受取ることができます。電子情報の全体が再生できるようなる。したがって、予め電子割符処理をした電子情報を配布しておいて、実際に利用するときに通信網を利用して容量の小さな配列情報あるいは残余の情報ブロックを送信することによって、実物の性能を提示・宣伝すると共に、正当な購入者以外には電子情報の利用ができない安全な電子情報送信システムを構築することができます。

【0012】

なお、配列情報は情報ブロックごとに付属させるヘッダに埋込んで送信するようにしてもよい。

配列情報を配布しておく場合にも、電子情報の復元に必要な情報ブロックが全て入手でき、ヘッダの復元ができなければ電子情報復元ができないため、真正の需用者でない者が盗用することを排除することができます。なお、一部の情報ブロックを発信元に保留しておく場合は情報の安全性がさらに高い。

【0013】

【発明の実施の形態】

以下、本発明の電子情報送信システムを実施例に基づき図面を参照して詳細に説明する。図1は本発明の電子情報送信システムの原理を説明するブロック図、図2は利用手順を説明するフロー図である。

本実施例の電子情報送信システムにおいて、発信元のコンピュータSは、小説・詩歌・日記・論説などの文学作品、映画、演劇、写真・絵画、音楽、ゲーム、コンピュータプログラム、研究論文、各種情報、その他、人が利用する各種のコンテンツを電子情報化した電

子情報Wを格納している。

【0014】

発信元コンピュータSは、電子情報Wを細かい情報エレメントEに分割し、任意に配列し直して複数の情報ブロックBに分配し、受信者のコンピュータRに送信する。情報ブロックBにおける情報エレメントEの順序は乱数的に決められて元の順序と関係がないため、そのままでは元の電子情報Wを復元することは困難である。特に、元の電子情報にダミー情報を付加し圧縮処理してから分割して分配したものでは、分割したときに作成する位置情報が無い限り元情報を推測することは不可能である。

また、発信元コンピュータSは、情報エレメントEの順序もしくは電子情報として再生するときに開始時刻から見た経過時間に関する情報を配列情報Aとして作成し、保存しておく。配列情報Aは、情報ブロックBにおける情報エレメントEの位置情報を含むものである。10

【0015】

情報ブロックBは色々な手段を用いて受信者のコンピュータRに供給することができます。たとえば、送信者のホームページに掲載しておいてインターネットを介して自由にダウンロードできるようにしておく。また、雑誌などに付録として添付したり、店舗に置いて自由に持帰れるようにしたり、ダイレクトメールで配布しても良い。

受信者は、入手した情報ブロックBをコンピュータRに取り込んで、電子情報の内容や性能を検討して入手したいと思ったら、購入する旨を発信元のコンピュータSに連絡する。発信元のコンピュータSは、購入意思を確認すると受信者のIDや決済方法など取引の安全を確認して、配列情報Aを受信者コンピュータRに送信する。20

【0016】

受信者コンピュータRは、必要なときに情報エレメントEを再統合して電子情報を復元するが、全体を一度に復元するのでは大容量のバッファが必要になるので、バッファメモリにはすぐに再生する部分のみを常時準備し、連続的に再生ができるようにする。しかし、復元処理が円滑に行かない場合にも情報の断絶が起らないようにして、看者に不自然な印象を与える不快な感じを生じさせないことが重要である。

受信者コンピュータRでは、所定の容量のバッファメモリMが準備されていて、5分間あるいは10分間など所定の時間は電子情報の流れが途切れても再生時の断続等がないようにしている。30

【0017】

図2は、再生時の手順を表す。再生の初期準備として、初めに所定時間分の電子情報を再生しバッファメモリMに格納する。電子情報の再生には、配列情報Aを発信元コンピュータSから取得し(S1)、取得した配列情報Aに基づき、初期の所定時間内に再生すべき電子情報を搭載した情報エレメントEが存在する情報ブロックBとその中における位置を知って、それらを収集する(S2)。

【0018】

収集した情報エレメントEを再生順に並べ戻して、電子情報を復元し、バッファメモリMに格納する(S3)。発信元コンピュータSに一部の電子情報が保留されているときや、中継放送など事象の発生について電子情報が形成されるときなど、復元に必要な情報が発信元コンピュータSに残っている場合は、これを取寄せて使用する。発信元コンピュータSが自発的に供給することもできる。40

【0019】

なお、秘密分散法の1種と見ることができる電子割符処理では、平文の前にダミー情報を乱数を追加し圧縮符号化して得た符号語を乱数データでマスク処理した後、乱数を用いてビット単位で適当数の割符に割振り送信または配布する。マスク処理した後の符号語の各ビットがどの割符に含まれているかを示す対応表をつくり各割符のヘッダに添付して送信または配信する。受信者側では、割符化の手順を逆にたどることによって、平文に戻して利用する。

したがって、電子情報は、割符化された情報ブロックを関連した部分について全て収集し50

ないと復元できない。

配列情報Aは、対応表と関連して作成されるが、分割された情報ピットについてその順序に基づき再生時にあいて何時必要となる部分かを示す情報であって、上記の電子割符処理に必須のものではない。

【0020】

所定量の電子情報が蓄積されたり、バッファメモリMから電子情報を読み出してディスプレードやスピーカを利用して再生を開始する(S4)。

その後は、上記所定量の電子情報がバッファメモリMにいつでも蓄積されているように、次の時間帯に対応する電子情報が搭載されているはずの情報エレメントEを、配列情報Aに基づいて収集し(S5)、電子情報を復元してバッファメモリMに追加する(S6)。 時間が経過するにつれて、バッファメモリMに格納された電子情報を読み出して再生し(S7)、電子情報が尽くるまで(S8)次のタイミングに来る情報エレメントEを収集しては復元しながらコンテンツの再生を続ける。

10

【0021】

このように、本実施例の電子情報送信システムでは、電子割符として分割された情報エレメントを時間の経過に沿って必要な部分を所定時間分だけ先行して収集し復元しておくので、看者は通常の映画やテレビ放送を見るようにあるいはレコード演奏を聞くように、電子情報コンテンツについて断裂等のない自然な再生により楽しむことができる。

なお、本実施例の電子情報送信システムは、インターネットテレビのように電子情報を逐次供給しながら再生させるストリーミング技術を使用する場合にも利用が可能で、電子割符技術を利用した安全な情報送信を行うことができる。

20

【0022】

【発明の効果】

以上詳細に説明した通り、本発明の電子情報送信システムによれば、動画等の時間に従って展開する大量の電子情報を送信するときに、秘密分散を用いて保管あるいは送信中にあけるデータの漏洩を防止し、再生を要求する者に対してが断裂等のストレスを最小限の抑制して動画等の再生を行うことができる。

【図面の簡単な説明】

【図1】本発明の電子情報送信システムの1実施例における原理説明図である。

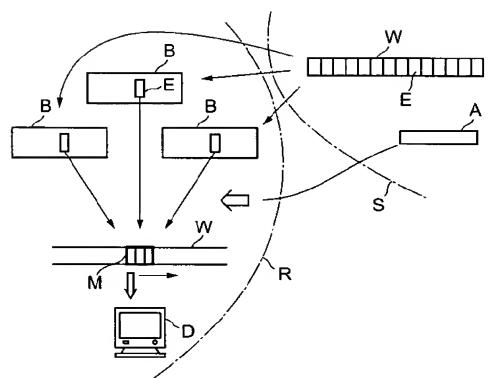
【図2】本実施例における受信者側の利用方法を説明するフロー図である。

30

【符号の説明】

- A 配列情報
- B 情報ブロック
- D ディスプレー
- E 情報エレメント
- M バッファメモリ
- R 受信者コンピュータ
- S 送信元コンピュータ
- W 電子情報

【図1】



【図2】

